UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

JÚLIA MACHADO DA ROSA

SEGURANÇA CIBERNÉTICA EM SUBESTAÇÕES DE ENERGIA

PORTO ALEGRE
1/2021

JÚLIA MACHADO DA ROSA

SEGURANÇA CIBERNÉTICA EM SUBESTAÇÕES DE ENERGIA

Projeto de diplomação do curso de engenharia elétrica da Universidade Federal do Rio Grande do Sul, apresentado como requisito parcial para a obtenção do Título de Engenheira Eletricista.

Orientador: Prof. Dr. Luiz Tiarajú dos Reis Loureiro

PORTO ALEGRE

2021

JULIA MACHADO DA ROSA

SEGURANÇA CIBERNÉTICA EM SUBESTAÇÕES DE ENERGIA

Projeto de diplomação apresentado como requisito parcial para a obtenção do título de Bacharel em Engenharia Elétrica pela Universidade Federal do Rio Grande do Sul.

Aprovado em: 29 de novembro de 2021

Banca Examinadora

Prof. Dr Tiarajú dos Reis Loureiro
Universidade Federal do Rio Grande do Sul

Prof. MSc Alexandre Ambrozi Junqueira
Universidade Federal do Rio Grande do Sul

Prof. Dr Roberto Petry Homrich
Universidade Federal do Rio Grande do Sul

Dedico este trabalho aos meus adorados irmãos Marina e Carlos Eduardo.

AGRADECIMENTOS

Aos meus pais, por nunca terem medido esforços para que eu alcançasse meus objetivos. Aos meus irmãos, pelo companheirismo, pela cumplicidade e pelo apoio em todos os momentos delicados da minha vida. À minha namorada Daniela por seu carinho, respeito e compreensão. Aos meus tios por serem grandes exemplos de força, resiliência e determinação.

“O que prevemos raramente ocorre; o que menos esperamos geralmente acontece.”
Benjamin Disraeli

RESUMO

Este trabalho traz uma análise das desvantagens trazidas aos sistemas de proteção e controle pela adoção de sistemas de automação de subestações quanto aos possíveis ataques cibernéticos. Estão descritos os principais componentes utilizados na elaboração de projetos de automação e os principais protocolos de comunicação adotados em subestações de energia. Por fim, é elaborado um estudo de caso no qual é proposta uma arquitetura de comunicação resiliente frente a possíveis ataques cibernéticos.

Palavras-chave: Segurança cibernética. Subestação. Automação.

ABSTRACT

This work presents an analysis of the disadvantages brought to protection and control systems by the adoption of substation automation systems regarding possible cyber attacks. The main components used in the elaboration of automation projects and the main communication protocols adopted in power substations are described. Finally, a case study is prepared in which a resilient communication architecture against possible cyber attacks is proposed.

Keywords: Cybersecurity. Substation. Automation.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ANEEL	Agência Nacional de Energia Elétrica
CLP	Controlador Lógico Programável
DJ	Disjuntor
DoS	*Denial of Service*
IEC	*International Electrotechnical Commission*
IED	*Intelligent Electronic Device*
IHM	Interface Homem-Máquina
LAN	*Local Area Network*
ONAN	Óleo Natural - Ar Natural
ONAF	Óleo Natural - Ar Forçado
ONS	Operador Nacional do Sistema
OSI	*Open System Interconnection*
PR	Para Raios
RCA	Relé de Proteção e Controle Alternado
RCP	Relé de Controle Principal
RPCA	Relé de Controle Alternado
RPCP	Relé de Proteção e Controle Principal
SAS	Sistema de Automação de Subestações
SCADA	*Supervisory Control And Data Acquisition*
SE	Subestação
SECC	Seccionadora
SEL	*Schweitzer Engineering Laboratories*
SIN	SISTEMA INTERLIGADO NACIONAL
TC	Transformador de Corrente
TPC/IP	*Transmission Control Protocol/Internet Protocol*
TP	Transformador de Potencial
WAN	*Wide Area Network*
UTR	Unidade Terminal Remoto

SUMÁRIO

1 INTRODUÇÃO

O objetivo de sistemas elétricos de potência é gerar e fornecer energia elétrica para os consumidores. Ter um sistema com faltas frequentes ou prolongadas numa sociedade amplamente dependente deste serviço é praticamente inconcebível e ocasionaria colapsos na rotina de todos os setores da sociedade.

No início do século XX a crescente dependência de energia elétrica trouxe a necessidade de se aumentar a confiabilidade do sistema. Neste período, as subestações eram controladas e monitoradas localmente, ou seja, o sistema elétrico era composto por inúmeras plantas de geração isoladas e suas cargas locais com pouca ou quase nenhuma possibilidade de comando e monitoramento remoto. O aumento da dependência gerou investimentos em plantas de geração e interconexão das linhas de transmissão para aumentar a confiabilidade do sistema através da redundância de fornecimento e elevação das tensões de transmissão para que a potência gerada pudesse ser transmitida a cargas mais distantes.

As subestações instaladas neste sistema mais interligado contavam com técnicos de operação alocados para atender as necessidades de manobra ou eventuais problemas técnicos mais rapidamente. A demanda por um sistema elétrico mais confiável e o aumento dos custos operacionais de manter um corpo de funcionários alocados nas subestações gerou uma busca por alternativas de monitoramento a distância de modo que um mesmo grupo de funcionários fosse capaz atender a diversas instalações. Na década de 1930 surgiu o primeiro sistema supervisório denominado SCADA - *Supervisory Control And Data Acquisition*.

Os primeiros sistemas *SCADA*, basicamente telemétricos, informavam periodicamente o estado das correntes elétricas do processo, monitoravam os sinais representativos e estados dos equipamentos primários. As informações obtidas eram disponibilizadas através de um painel de lâmpadas e indicadores, sem a necessidade de interferência operacional.

Em se tratando das funções de proteção implementáveis numa mesma instalação, neste período, eram limitadas devido aos custos envolvidos, tanto para instalação quanto para manutenção ou ampliação.

Todo comando dado aos equipamentos primários envolvia uma quantidade considerável de cabos de cobre e contatos pertencentes a dispositivos auxiliares, chaves seletoras, lâmpadas de indicação e medidores de grandezas analógicos.

Todas as lógicas de intertravamentos necessárias para o pleno funcionamento das transferências de cargas e manobras da subestação eram do tipo “lógica de relé” realizados com conexões físicas dos contatos, em série ou paralelo, através de cabos de cobre. Subestações de médio ou grande porte podiam requerer até centenas de quilômetros de cabos.

As funções de proteção existentes eram realizadas através de relés eletromecânicos. Os relés eletromecânicos eram unifuncionais, ou seja, tinham capacidade de executar apenas uma função de proteção, fator que limitava a proteção aplicável num mesmo módulo da subestação, visto que estes equipamentos exigiam painéis de proteção e controle maiores e consequentemente um prédio de comando maior, além disso, uma maior quantidade de relés eletromecânicos acarretava num maior custo com cabeamento de cobre e estrutura civil para comportá-los.

Segundo KRIEG e FINN (2019), as informações obtidas pelos relés eletromecânicos estavam disponíveis localmente através do mostrador do medidor ou anunciador local e buzina para atrair a atenção do operador. O operador era em seguida, responsável por comunicar os eventos a outras partes interessadas.

Com o avanço tecnológico da eletrônica e dos microprocessadores, surgiram os primeiros equipamentos digitais a serem instalados nas subestações: as unidades terminais remotas - UTRs. Inicialmente as UTRs eram meros equipamentos de aquisição de dados (como estados dos equipamentos e seus alarmes indicativos de anormalidades) e envio de comandos, constituindo uma interface entre o processo elétrico e o sistema *SCADA*.

A utilização de UTRs permitiu que fossem criados os primeiros centros de operação de subestações nos quais toda a inteligência do sistema de supervisão e controle do processo elétrico eram instalados. Os centros de operação de subestações também possuíam poderosos computadores e IHM – Interface homem-máquina.

A evolução das UTRs trouxe a inteligência necessária para que estes equipamentos fossem capazes de realizar funções de autoteste, pré-processamento de dados de medição ou eventos, datação e registro de eventos.

Apesar da vantagem do microprocessador da UTR oferecer o potencial de aumento significativo nas funcionalidades sem gerar grandes custos este

equipamento digital foi aceito lentamente pelo setor elétrico de potência devido a questões de confiabilidade, ciclo de vida e resiliência.

Desde o início dos anos 2000, o uso de Dispositivos Eletrônicos Inteligentes (IEDs) tem sido cada vez maior nas subestações uma vez que agregam cada vez mais funções, permitindo uma redução nos custos de implantação, manutenção e no número de cabos e equipamentos necessários à sua utilização. Os IEDs proporcionam a troca de informações mais rápidas e em maior quantidade, agregando maior confiabilidade ao sistema, além de simplificar o projeto e permitir a sincronização de tempo entre os dispositivos (LACERDA e CARNEIRO, 2010).

A figura 1 ilustra três relés de proteção diferencial. A principal diferença é que no relé digital (IED) a função diferencial não é a única disponível, este equipamento, conforme mencionado anteriormente, pode executar funções de sobrecorrente, subtensão, sobretensão, falha disjuntor.

Figura 1. Relé eletromecânico versus Relé Estático versus Relé Digital

Fonte: (COVRE, 2011)

A popularização dos IEDs no sistema elétrico trouxe outra mudança tecnológica significativa uma vez que os protocolos de comunicação *SCADA* existentes eram proprietários, ou seja, cada fabricante tinha os seus próprios protocolos e requisitos de comunicação, surgiu uma tendência no sentido de incentivar a criação de um protocolo aberto e padronizado. O resultado da tendência de padronização trazida pelos IEDs são as normas IEC 60870-5 (1995), consolidação dos tradicionais protocolos *SCADA* orientados a lista de pontos, e a IEC 61850 (2004), primeiro protocolo *SCADA* orientado a objeto.

O avanço tecnológico computacional permitiu que as funções de controle, medição, oscilografia que é o registro das oscilações das grandezas elétricas, registro de eventos e localização de falta fossem adicionados aos IEDs tornando-os poderosos

equipamentos multifuncionais. Além disso, permitiu que diversas funções de proteção, antes desempenhadas por diferentes relés, fossem agregadas num mesmo *hardware*, reduzindo o número de equipamentos necessários para implementação do sistema de proteção, bem como da infraestrutura necessária na subestação.

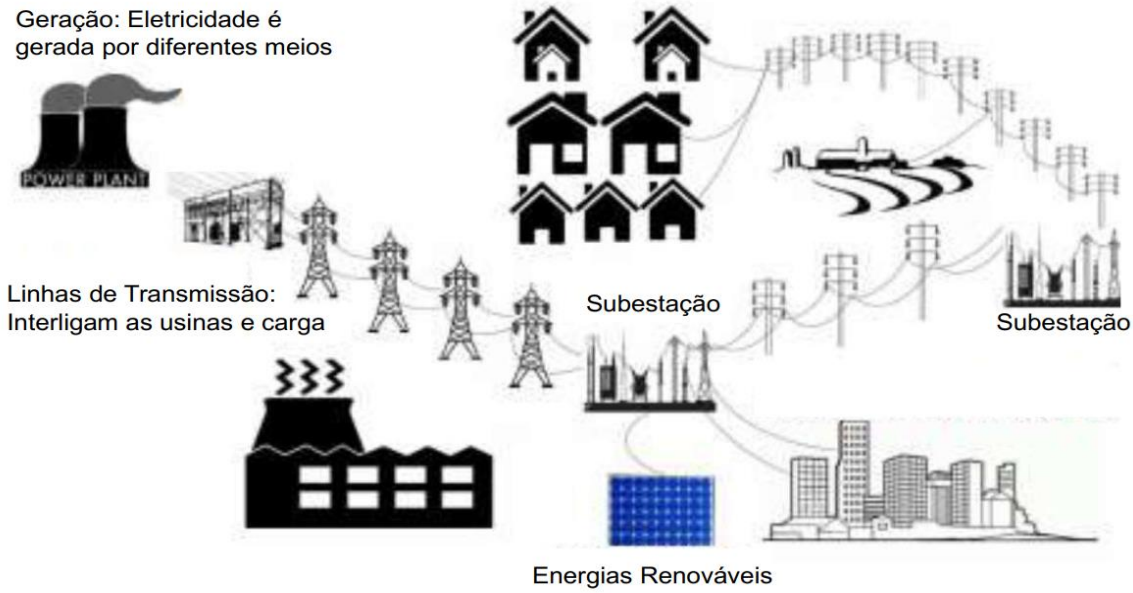
Comparando as arquiteturas existentes nas subestações onde são utilizadas UTRs ou IEDs, percebe-se grande diferença visto que num sistema baseado em UTRs a arquitetura é chamada concentrada, e num sistema baseado em IEDs é chamada distribuída. Arquitetura concentrada no sentido que um mesmo equipamento, neste caso UTR, concentra sinais oriundos de todos os módulos existentes na subestação enquanto que numa arquitetura distribuída são empregados um ou mais IEDs por módulo.

Apesar das inúmeras vantagens, os IEDs representam os maiores pontos de vulnerabilidade dentro do sistema de proteção devido a sua comunicação *ethernet*. O sistema *SCADA*, que faz a coleta de dados nas instalações e transmite aos centros de controle onde ocorre o processamento destes dados e comandos de proteção ou controle. A utilização de redes *ethernets* trouxe como desvantagem a ameaça de ataques cibernéticos para danificar ou sequestrar informações.

Segundo Dorothy (2017) existem três conceitos chaves que devem ser atendidos em todo sistema cibernético: confidencialidade, integridade e disponibilidade. Em Smart Grid, confidencialidade se refere a impor limites de acessos às informações pessoais dos consumidores que utilizam a tecnologia. Integridade se refere a proteger contra informações incorretas, alterações ou destruição, a fim de prevenir o rompimento dos dados e garantir a autenticidade e validade dos dados armazenados. Disponibilidade refere-se a garantir que um acesso confiável e oportuno é fornecido aos usuários autorizados e negado aos usuários não autorizados.

Subestações são o coração dos sistemas elétricos de potência, e a segurança da rede precisa ser feita primeiro ao nível das subestações. Uma subestação é exposta a uma ampla gama de ameaças, estas ameaças podem ser externas como um terrorista, espião ou *hacker*. Além disso, estas ameaças podem ser internas causadas por empregados insatisfeitos ou causadas inadvertidamente pela equipe de manutenção. (NOUH, 2018)

Figura 2. Estrutura do Sistema Smart Grid



Fonte: (DOROTHY, 2017)

Somente nos primeiros meses de 2021 duas empresas nacionais do setor de energia, Copel e Eletronuclear, relataram ter sofrido ataques cibernéticos através de *ransomware* (software malicioso que sequestra arquivos e bloqueia sistemas de um computador). Apesar de nenhum dos ataques ter causado desabastecimento de energia, estes acontecimentos aumentaram a discussão a respeito do tema. Em abril de 2021 a ANEEL abriu uma consulta pública visando discutir a regulamentação da blindagem cibernética no sistema elétrico. O objetivo desta será estabelecer diretrizes para arquitetura, gestão de acesso e de vulnerabilidades, inventário de ativos e resposta a incidentes cibernéticos.

Em fevereiro de 2018 foram divulgados dados referentes ao número de subestações de Distribuição e Transmissão em operação no Brasil. Quanto às subestações de Geração o órgão responsável, Superintendência de Fiscalização dos Serviços de Geração (SFG), não soube precisar um número, porém fez uma estimativa baseada nas seguintes premissas:

a) Em geral, as centrais geradoras possuem uma subestação de conexão à rede de distribuição e/ou transmissão;

b) algumas usinas possuem mais de uma subestação de conexão;

c) algumas usinas classificadas como autoprodutor possuem subestações apenas para uso exclusivo;

d) algumas usinas, principalmente de pequeno porte, possuem conexão interna ou externa feita apenas através de transformadores, não sendo esses propriamente subestações.

Dessa forma foi inferido que o número de subestações de geração seja aproximadamente o número de centrais geradoras em operação no país, que à época era de 4.905, de acordo com consulta feita ao Banco de Informações de Geração (BIG) da ANEEL.

Quadro 1. Subestações em Operação no Brasil

MODALIDADE DA SUBESTAÇÃO	QUANTIDADE
Geração	4905
Transmissão	576
Distribuição	5775

Fonte: Autora

Para atender à crescente demanda por energia elétrica de qualidade, aliada a uma indispensável boa gestão empresarial com práticas em redução de custos, as concessionárias têm direcionado parte de seus investimentos à automação de suas instalações. O relatório de análises divulgado pela ANEEL em 2016 cita que entre os anos de 2013 a 2016, nas instalações de transmissão do sistema elétrico, houve uma taxa de crescimento médio de 45 novas instalações teleassistidas por ano culminando na proporção de 82% das concessionárias se utilizando da operação de forma remota em seus ativos.

Tendo em vista o montante de subestações operando de modo teleassistido atualmente no país, que num futuro próximo este número seja praticamente igual ao total de instalações existentes e que apesar dos inúmeros benefícios que o emprego da tecnologia oferece pode-se prever um cenário crítico em relação à cibersegurança.

Segundo o *Global Energy Institute*, a segurança cibernética se tornou uma das principais ameaças à infraestrutura de energia dos Estados Unidos. Embora a Internet tenha servido para aproximar o mundo, ela também pode ser usada para lançar ataques remotos contra a infraestrutura de energia. Os esforços dedicados à segurança cibernética da rede elétrica e outros sistemas de distribuição de energia tornaram-se as principais preocupações do setor.

Para KUNSMAN e BRAENDLE (2010), o princípio mais importante de qualquer de arquitetura de segurança é a defesa em profundidade. Ter uma única

camada de defesa raramente é suficiente, pois qualquer mecanismo de segurança pode ser superado por um invasor. Deste modo manter uma defesa em múltiplas camadas na qual as informações mais importantes estejam em camadas mais profundas é o mais próximo ao ideal.

2 SUBESTAÇÕES DE ENERGIA

Segundo Mamede (2021), o sistema elétrico de potência é formado por três segmentos: geração, transmissão e distribuição. Para que a energia gerada no primeiro segmento chegue ao consumidor que está ligado ao sistema de distribuição, é necessário que exista em cada um destes segmentos uma subestação de energia para elevar ou reduzir as tensões a diferentes níveis.

Uma subestação de energia é constituída por diversos circuitos de linhas de transmissão (em corrente contínua ou corrente alternada) que são conectadas aos barramentos por meio de chaves seccionadoras e disjuntores. O arranjo físico adotado numa subestação, depende do nível de tensão da mesma, da flexibilidade operacional e dos requisitos de confiabilidade.

Cabe salientar que o arranjo de barramento definido dita a complexibilidade do sistema de proteção e controle a ser empregado.

2.1 Categorias de Utilização

2.1.1 Subestação Elevadora

Essa categoria de subestação eleva o nível da tensão gerada por uma fonte de energia para que esta potência possa ser transmitida por linhas de transmissão com tensões mais elevadas do que a tensão de origem. Essas subestações normalmente são instaladas próximos a usinas fotovoltaicas, elétricas, térmicas, hidrelétricas, etc.

2.1.2 Subestação Abaixadora

O objetivo dessa categoria de subestação é reduzir o nível de tensão e distribuir a potência associada no segmento de distribuição, sejam redes aéreas ou subterrâneas, alimentando subestações com níveis de tensões mais baixos.

Normalmente são instaladas em regiões distantes dos centros urbanos para evitar que linhas de transmissão de tensões elevadas, por exemplo: 230 kV, 525 kV, 750 kV gerem transtornos pela ocupação dos espaços urbanos ou mesmo pelos campos elétricos e magnéticos associados.

2.1.3 Subestação de Distribuição

São muito comuns. Destinadas a reduzir os níveis de tensão visando atender as necessidades das concessionárias, permissionárias ou consumidores de médio porte.

2.1.4 Subestação de Manobra

Normalmente são subestações pertencentes ao SIN – Sistema Interligado Nacional e a Rede Básica. Sua principal função é o chaveamento das linhas de transmissão de tensões entre 230 kV a 750 kV. Contudo, também é possível encontrar esta categoria de subestações sendo empregadas nos segmentos de distribuição e subtransmissão.

2.1.5 Subestação Conversora

Nos casos onde há necessidade de transmitir grandes quantidades de energia entre duas regiões muito distantes costuma ser economicamente viável a implantação de linhas de transmissão em corrente contínua, visto que esse modo de transmissão diminui o custo de implantação das linhas e perdas energéticas envolvidas na transmissão, de modo que cobrem os custos envolvidos na implantação das subestações inversoras e conversoras, tornando esse modo transmissão vantajoso.

2.1.6 Subestação Móvel

Muito aplicada nos segmentos de distribuição e subtransmissão, esta categoria tem por objetivo atender as situações emergenciais. Normalmente é montada sobre um veículo motorizado possibilitando o atendimento de diversas instalações, a depender da necessidade.

2.2 Formas de Operação

2.2.1 Subestações com Operação Presencial

São subestações com operação presencial exigem a presença de um ou mais operadores revezando por turnos. O número de operadores trabalhando simultaneamente é definido pela complexidade da instalação. Segundo Mamede (2021) este tipo de subestação está migrando para sistemas com tecnologias mais avançadas que permitem a operação de modo remoto.

2.2.2 Subestações Supervisionadas

Quanto ao sistema de proteção e controle das subestações convencionais e subestações automatizadas existem diferenças significativas. Dada a tendência de migração observada nas últimas décadas para sistemas de proteção e controle automatizados pode-se citar como principais desvantagens do sistema convencional o grande número de relés auxiliares, chaves seletoras e temporizadores necessários, quantidade de circuitos necessários para elaboração de lógicas operacionais e de intertravamento (acarretando numa infraestrutura civil custosa visto a quantidade de cabos). Em subestações automatizadas a troca de informações pode ser realizada através de rede de comunicação ou através de lógicas internas programadas nos IEDs, reduzindo consideravelmente o número de relés auxiliares e dispositivos. Não exigem a presença de operadores na instalação.

2.3 Principais Equipamentos Primários

2.3.1 Para-Raios

Figura 3. Para Raios

Fonte: (Mamede, 2013)

Os para-raios são utilizados para proteger os diversos equipamentos que compõem uma subestação de potência ou simplesmente um único transformador de

distribuição instalado em poste. Os Para-Raios limitam as sobretensões a um valor máximo. Esse valor é tomado como nível de proteção que o Para-Raios oferece ao sistema.

Para que se protejam os sistemas elétricos dos surtos de tensão, que também podem ter origem durante manobras de chaves seccionadoras e disjuntores (sobretensões de origem térmica) são instalados equipamentos apropriados que reduzem o nível de sobretensão a valores compatíveis com a suportabilidade desses sistemas. (Mamede, 2013)

O elemento constituinte mais importante do Para-Raios é o resistor de característica não-linear, atualmente, são utilizados carbonato de silício ou óxido de zinco.

2.3.2 Transformador de Corrente

Figura 4. Transformador de Corrente

Fonte: (Mamede, 2013)

Os transformadores de corrente são equipamentos que permitem aos instrumentos de medição e proteção funcionar adequadamente sem que seja necessário possuírem correntes nominais de acordo com a corrente de carga do circuito ao qual está ligado. Na sua forma mais simples eles possuem corrente nominal

transformada é, na maioria dos casos, igual a 5A. Desta forma, os instrumentos de medição e proteção são dimensionados em tamanhos reduzidos com as bobinas de corrente constituídas de poucos fios de cobre.

Transformadores de corrente são utilizados para suprir aparelhos que apresentam baixa resistência elétrica, tais como: amperímetros, relés, medidores de energia, medidores de potência, etc. (Mamede, 2013)

2.3.3 Transformador de Potencial

Figura 5. Transformador de Potencial

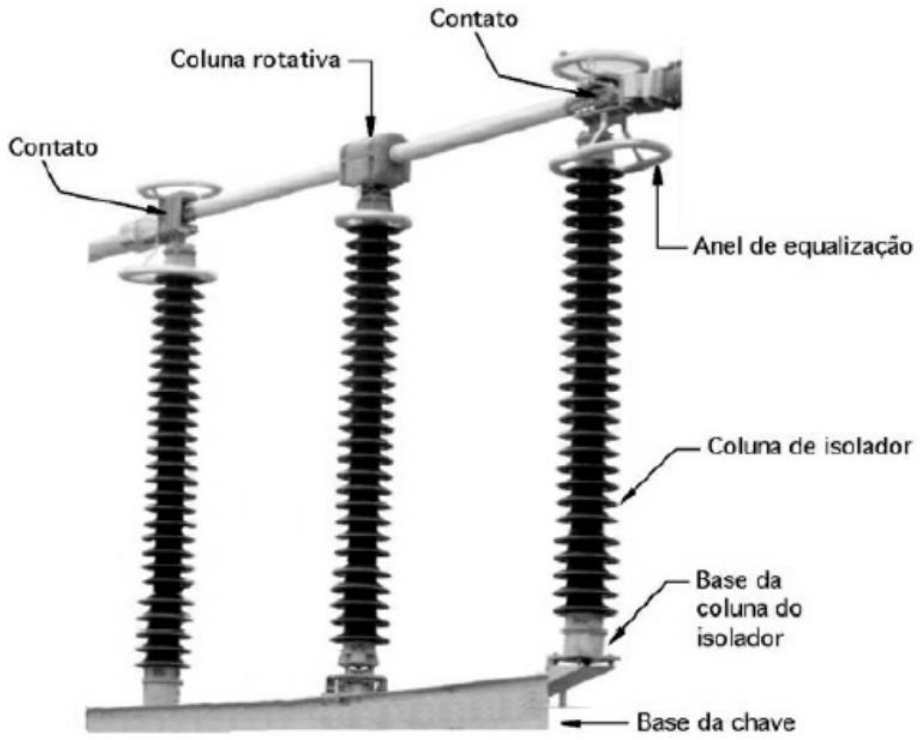
Fonte: (Mamede, 2013)

Segundo Mamede (2013), os transformadores de potencial são equipamentos que permitem aos instrumentos de medição e proteção funcionarem adequadamente sem que seja necessário possuírem tensão de isolamento de acordo com a da rede a qual estão ligados.

Na sua forma mais simples os transformadores de potencial possuírem enrolamentos primários de muitas espiras e um enrolamento secundário através do qual se obtém a tensão desejada, normalmente padronizada em 115 V ou 115/√3 V. Desta forma, os instrumentos de proteção e medição são dimensionados em tamanhos reduzidos com bobinas e demais componentes de baixa isolação.

2.3.4 Seccionadora

Figura 6. Seccionadora



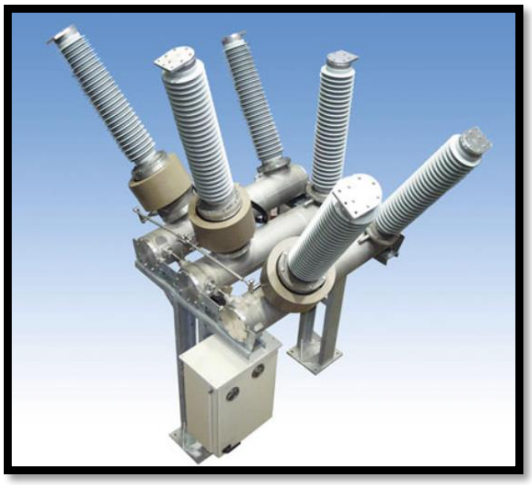
Fonte: (Mamede, 2013)

Seccionadoras são utilizadas numa subestação de energia para permitir manobras de circuitos elétricos, sem cargas, isolando disjuntores, transformadores de medida e de proteção barramentos. As seccionadoras podem ser fabricadas em unidades monopolares ou tripolares, em subestações de alta tensão, normalmente se empregam seccionadoras tripolares. É recomendado que uma chave seccionadora seja operada sem carga para não colocar em risco seus contatos e reduzir sua vida útil. A exceção é quando são previstas pequenas correntes de magnetização oriundas de transformadores de potência ou correntes capacitivas.

Dentre as principais funções de uma seccionadora estão a manobra de circuitos, para transferência de cargas e isolamento dos equipamentos para permitir serviços de manutenção.

2.3.5 Disjuntor

Figura 7. Disjuntor



Fonte: (Krieg e Finn, 2019)

Os disjuntores são equipamentos destinados a interrupção e reestabelecimento das correntes elétricas num determinado ponto do circuito. (Mamede, 2013)

A principal função de um disjuntor é interromper as correntes de defeito de um determinado circuito num tempo menor do que 2 ciclos de onda. Porém, esta não é sua única aplicação, o disjuntor também pode operar interrompendo correntes a plena carga e a vazio que estejam numa situação normal apenas por necessidade de manobra de cargas.

Apresentam uma variedade de sensores e dispositivos instalados com o objetivo de monitorar estado e saúde dos circuitos internos do equipamento e de suas partes constituintes, por exemplo: supervisão das bobinas de abertura e fechamento, subtensão nos circuitos de comando e motor, supervisão de estado da mola de fechamento, contatos auxiliares de estado e pressão do gás (nos disjuntores isolados a gás).

Numa manobra de abertura, os contatos primários do disjuntor se separam, um arco elétrico se estabelece e a corrente irá continuar a fluir através desse arco até que a onda de corrente passe pelo zero, reduzindo a temperatura e a ionização interrompendo a passagem de corrente. Uma das técnicas de extinção do arco causado pela abertura do disjuntor é substituir o meio ionizado por gases inertes SF6 – hexafluoreto de enxofre, vácuo ou óleo mineral isolante com o objetivo aumentar a rigidez dielétrica deste meio.

2.3.6 Transformador de Potência

Figura 8. Transformador de Potência

Fonte: (Krieg e Finn, 2019)

Transformador é um equipamento de operação estática que por meio do princípio de indução eletromagnética transfere energia de um circuito, chamado primário, para um ou mais circuitos denominados, respectivamente, secundário e terciário, sendo, no entanto, mantida a mesma frequência, porém com tensões e correntes diferentes. Os transformadores de força são instalados nas subestações em que há trocas nos níveis de tensão.

Os transformadores de potência, por serem equipamentos de extrema importância numa instalação, são dotados de uma grande variedade de sensores que são responsáveis por fornecer aos sistemas de monitoramento informações sobre o estado do equipamento.

Dentre os principais dispositivos de monitoramento da saúde do transformador, estão o relé *Bucholz*, sensores de temperatura do óleo ou dos enrolamentos, dispositivos de alívio de pressão, sensor de ruptura de membrana, níveis mínimos e máximos de óleo, etc.

O relé *Bucholz* é um sensor que indica eventos internos ocorridos no transformador através do monitoramento do fluxo de gás originado no tanque principal do transformador.

3 AQUISIÇÃO E FLUXO DE DADOS DE SUBESTAÇÕES

3.1 Sinais Analógicos:

Dados analógicos compreendem todos sinais contínuos e variáveis no tempo. No contexto de subestações são obtidos através dos transformadores de instrumentos que reduzem os valores de potencial e corrente presentes em determinado módulo da ou barramento da subestação. Esses dados adquiridos são convertidos em transdutores em sinais de corrente que varia entre 4-20 mA.

3.2 Sinais Digitais:

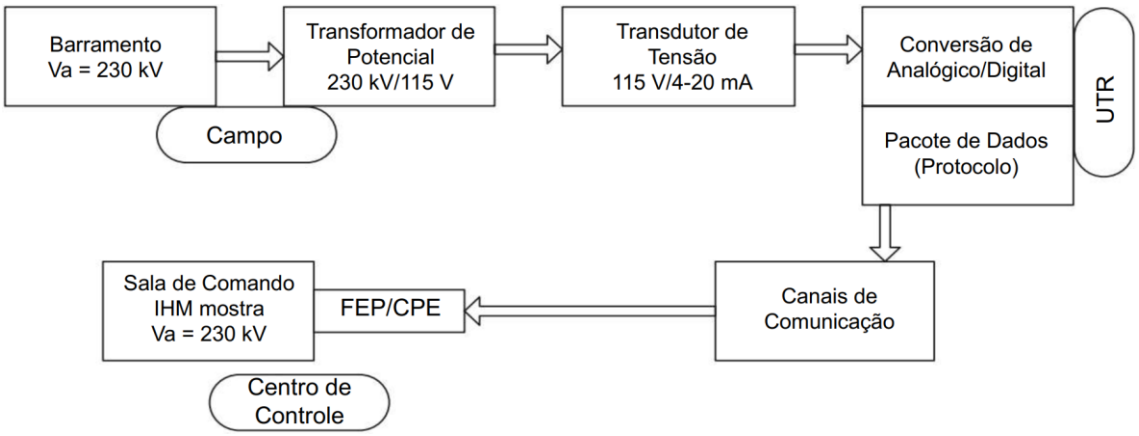
Um sinal digital é descontínuo se altera entre um estado e outro através de etapas discretas, geralmente é representado em binário, ou em dois níveis: baixo e alto. Os sinais digitais incluem os alarmes dos sensores internos dos equipamentos e sinais que indicam o estado (aberto/fechado).

3.3 Fluxo de Dado do Equipamento à IHM

O fluxo de dados dentro do sistema *SCADA* pode ser descrito analisando o fluxo de um sinal analógico obtido no pátio da subestação transmitido à tela da IHM, conforme ilustrado na figura 9. Nesse exemplo, existe um barramento operando sob a tensão de 230 kV e conectado a ele está um transformador de potencial que faz a conversão de 230 kV/115 V. Este sinal de analógico de tensão é convertido por um transdutor de tensão para um sinal analógico de corrente que varia entre 4-20mA. Na entrada analógica da UTR este sinal é convertido em dado digital. Além disso, o sinal digital obtido é transmitido, de acordo com o protocolo existente, à IHM. Na IHM, os pacotes são recebidos pelo processador, decodificados e os dados são recuperados. Os dados são escalados proporcionalmente até a faixa de 230 kV e exibidos no diagrama unifilar do console do operador completando o ciclo de monitoramento.

A mesma sequência pode ser reconstituída da IHM para o campo, no caso de um comando de controle emitido pelo operador, a ser executado no campo. O uso de UTR com entradas/saídas e comunicações seriais, uma vez predominante com todos os equipamentos de campo, fez a transição para concentradores de dados que se comunicam com IEDs com comunicações digitais em rede. (Thomas e McDonald, 2015)

Figura 9. Transferência de Dados do Barramento a IHM



Fonte: (Thomas e McDonald, 2015)

Nas instalações em que há controle e supervisão através de IEDs existe a possibilidade de se comunicar diretamente com a unidade concentradora, dependendo da arquitetura, serial ou *ethernet*, e meio de comunicação definidos, por exemplo: RS 232, RS 485, UTP.

4 SISTEMA DE AUTOMAÇÃO DE SUBESTAÇÕES

Os sistemas de automação têm se popularizado devido a capacidade de adquirir, analisar e executar ações de operações na ordem de milissegundos. Dentre as principais facilidades e funcionalidades contidas num sistema automatizado estão as seguintes:

- A seleção de abertura e fechamento de disjuntores e chaves seccionadoras;
- Bloqueio e liberação de manobras de transferência de cargas;
- Disponibilizar na IHM o estado de cada chave seccionadora e disjuntor;
- Disponibilizar na IHM os valores analógicos de tensão, corrente, potência e fator de potência;
- Disponibilizar na IHM resultados de alarmes dos equipamentos;
- Monitorar a integridade dos IEDs de proteção;
- Monitorar a integridade dos circuitos de serviços auxiliares.

Na maioria dos casos, o sistema de automação da subestação permite três níveis de operação (pontos de interface homem-máquina). No entanto, o número de níveis empregados dependerá da prática local e pode ser restrito aos primeiros dois níveis de controle.

- Nível de processo

O nível de processo compreende os equipamentos primários. Nos equipamentos primários destinados a manobra ou comutação de circuitos é comum que existam chaves seletoras que permitem a operação dos equipamentos nos modos local ou remoto.

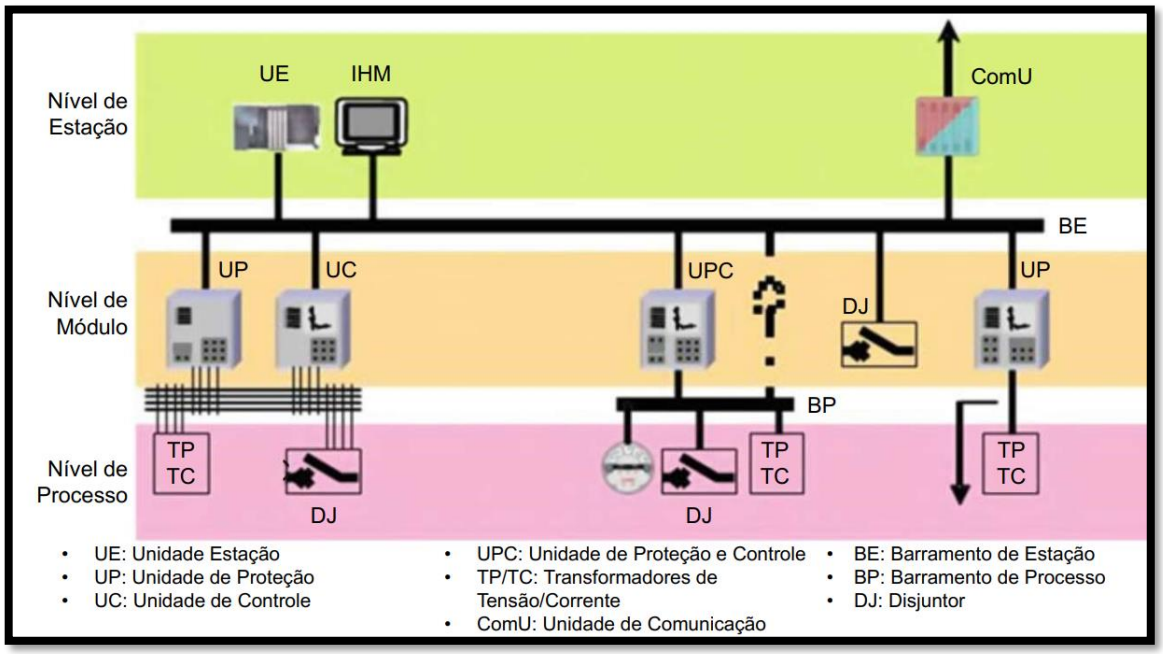
- Nível de módulo

Neste nível, encontram-se os dispositivos de supervisão, controle e proteção dos módulos.

- Nível de estação

É o nível de interface com o sistema *SCADA*. Compreende a IHM (interface homem-máquina), que permite operação local, e *Gateways* para troca de informações e comandos com o centro de operação de subestações.

Figura 10. Níveis de Operação



Fonte: (KRIEG e FINN, 2019)

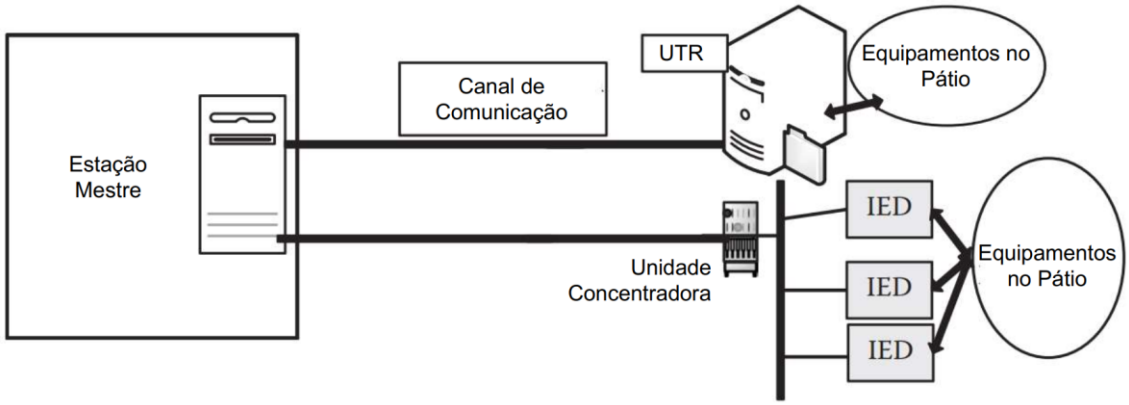
Apenas um nível de operação pode comandar simultaneamente e a definição das regras para mudança no modo de operação é definida pelo usuário. Mas geralmente a seleção é entre os níveis de operação e de módulo.

Segundo KRIEG e FINN (2019) nos últimos anos, o tema das comunicações tanto quanto externa, ou seja, entre as subestações ou entre a subestação e centro de operação de subestações tornou-se cada vez mais importante.

A comunicação tornou-se uma atividade consolidada graças aos altos investimentos das concessionárias de energia em suas próprias infraestruturas de telecomunicações dedicadas. A proteção do sistema de energia impõe os mais rigorosos requisitos de desempenho em um sistema de telecomunicações dedicados exigindo a extinção de falhas em 80-100 ms. Além disso, os requisitos de disponibilidade e integridade da rede são muito além daqueles de um serviço de telecomunicações convencional e continuam a tornar-se cada vez mais exigentes.

O sistema de comunicação interno da subestação é composto por Unidades Terminal Remoto (UTR), Controladores Lógicos Programáveis (CLP) e IEDs que disponibilizam as informações às partes interessadas na Estação Mestre.

Figura 11. Componentes do Sistema SCADA



Fonte: (Thomas e McDonald, 2015)

4.1 UTR (Unidade Terminal Remoto)

É um dispositivo eletrônico microprocessado responsável por fazer a interface entre os equipamentos da subestação e o *SCADA*. A UTR adquire os dados de campo dos diferentes equipamentos presentes no pátio, processa e transmite os dados relevantes aos centros de operação.

4.2 CLP (Controlador Lógico Programável)

É um computador digital usado para automação de processos eletromecânicos. Ao contrário dos computadores de uso geral, eles são projetados para múltiplas entradas e saídas, operação em faixas de temperatura estendidas, para ser imune a ruído elétrico e ser resistente a vibração e impacto. Programas para controlar as operações do processo são geralmente armazenadas em memória não volátil ou com bateria de apoio.

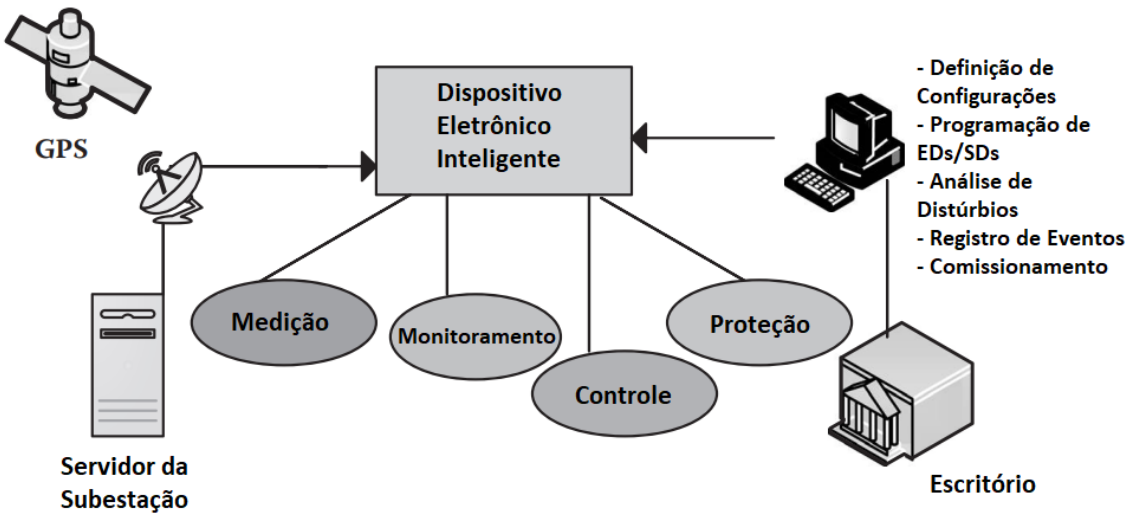
4.3 IED (Dispositivo Eletrônico Inteligente)

A definição padrão da indústria de um IED é “Qualquer dispositivo que incorpore um ou mais processadores com capacidade de receber ou enviar dados/controle de ou para uma fonte externa (por exemplo, medidores multifuncionais eletrônicos, relés digitais e controladores)." Os IEDs foram amplamente implantados em sistemas de automação de energia recentemente, e a mudança de UTRs para IEDs é evidente devido à integração e recursos de interoperabilidade dos IEDs. (Thomas e McDonald, 2015)

A figura 12 apresenta o diagrama de blocos de um IED e através desta percebe-se que este dispositivo é polivalente, de natureza modular, flexível, adaptável

e possui uma robusta capacidade de comunicação. Nos seus recursos de comunicação existe a possibilidade de seleção entre vários protocolos de envios e recebimentos de dados. IEDs possuem alta taxa de processamento de dados para realização de inúmeras funções de proteção, medição e armazenamento de eventos (útil para análises pós-eventos).

Figura 12. Diagrama de Blocos de um IED



Fonte: (Thomas e McDonald, 2015)

Além disso, o IED traz recursos adicionais, como monitoramento de circuito externo, sincronização em tempo real do evento, acesso aos dados locais e da subestação, controlador lógico programável e toda uma gama de ferramentas de software para comissionamento, testes, relatórios de eventos e análise de falhas. (Thomas e McDonald, 2015)

4.4 IHM (Interface homem-máquina)

A interface homem-máquina consiste de dispositivo que fornece as informações situacionais dos processos automatizados (alarmes, valores de processo e tendências) para o operador. O IHM pode operar em diferentes plataformas, mas no contexto das subestações, é utilizado um *desktop* instalado na sala de comando. Além disso, a IHM pode monitorar várias redes de processo.

4.5 Unidade Concentradora de Dados

Uma Unidade Concentradora de Dados une as informações e as disponibiliza a outros dispositivos. Esta concentração dos dados pode ser feita através de uma UTR, porém a principal diferença é que a UCD não tem interfaces físicas para

monitorar e executar comandos. As informações da UCD são obtidas a partir de protocolos de comunicação vindos de outro dispositivo em vez de uma conexão direta.

4.6 Switches Ethernet

Os *switches ethernet* são equipamentos que permitem a comunicação de dispositivos entre si. São muito aplicados nas Redes LAN - *Local Area Networks*, apesar de terem como desvantagem frente às comunicações por fibra óptica a interferência eletromagnética.

Os *switches* para aplicação em subestações são diferentes daqueles produzidos para aplicação comercial. A subestação é um ambiente hostil com extremos de temperatura, interferência eletromagnética e transientes de tensão exigindo que o equipamento tenha uma construção mais robusta e fontes de alimentação redundantes. Além disso, em subestações são utilizados somente *switches* gerenciáveis pois esses priorizam a comunicação.

4.7 Roteador

Os roteadores são equipamentos responsáveis por encaminhar os pacotes de dados para diferentes redes. Em subestações, os roteadores são frequentemente usados para criar perímetros de segurança nas LAN.

5 MODELOS E TOPOLOGIAS DE REDES

5.1 Redes LAN

As redes locais são redes privativas de comunicação na qual os equipamentos que a compõem estão instalados numa área limitada, no contexto das subestações estes equipamentos estão no prédio de comando.

A LAN é uma rede de comunicação de alta velocidade dentro da subestação e estendendo-se para o pátio de manobras. Ele transfere rapidamente os dados entre os IEDs. (Thomas e McDonald, 2015)

A maioria das redes LAN utilizam o padrão *ethernet*, que garante a troca de informações de modo confiável. A velocidade de transmissão varia entre 10 Mbits/s a 1 Gbits/s.

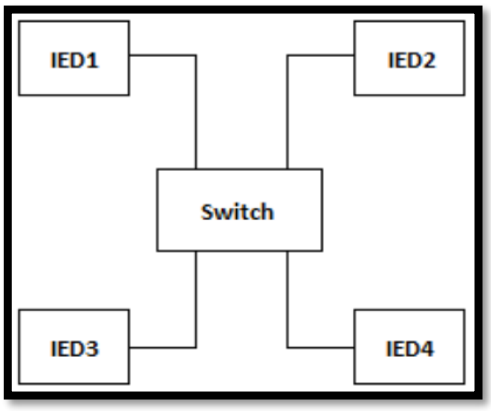
5.2 Redes WAN:

É uma rede de comunicação que contempla uma grande área geográfica, como cidades, estados e até países. Normalmente é resultado da união de redes menores, como várias LANs (redes locais). Ou seja, é uma rede de comunicação utilizada para interações entre subestações ou entre subestações e centros de operação de subestações. O meio físico é fibra óptica.

5.3 Topologia em Estrela

As topologias em estrela são simples. Eles oferecem tempos de transmissão muito reduzidos. Infelizmente, eles também resultam em um único ponto de falha, o centro da estrela. Por esse motivo, a topologia em estrela não é popular em instalações críticas. (McDonald, 2012)

Figura 13. Topologia de Rede Estrela



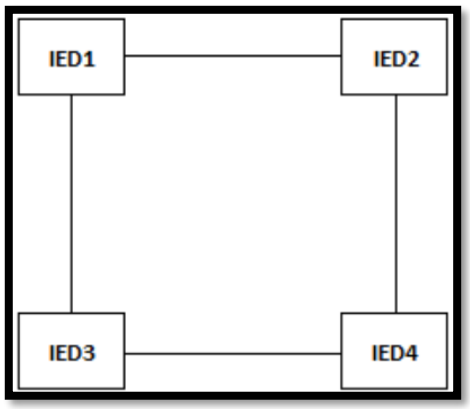
Fonte: (KREUTZ, 2014)

As principais vantagens da aplicação dessa topologia são que numa situação de falha em algum dos cabos que interligam o *switch* ao IED essa falta é isolada não acarretando em falhas nos demais IEDs e a facilidade de expansão, pois caso não tenha portas de conexão disponíveis basta substituí-lo. A principal desvantagem desta topologia é que um problema técnico no *switch* afeta todos os IEDs.

5.4 Topologia em Anel

As redes *ethernet* com topologia em anel são frequentemente preferidas em ambientes de subestação. As razões de seu sucesso estão relacionadas à redundância intuitiva e aos tempos de redirecionamento calculáveis e rápidos. A simplicidade da rede é atraente para manutenção e projeto. (McDonald, 2012)

Figura 14. Topologia de Rede em Anel



Fonte: (KREUTZ, 2014)

As vantagens desta topologia são a facilidade de instalação e reconfiguração, visto que cada dispositivo é interligado aos vizinhos imediatos. Um alerta é gerado se qualquer dispositivo não receber um sinal dentro de um período predeterminado, técnica que facilita o isolamento de uma falha. Como desvantagem tem-se a necessidade de paralisação da rede numa ampliação e que a falha em dois ou mais dispositivos afeta o restante da rede.

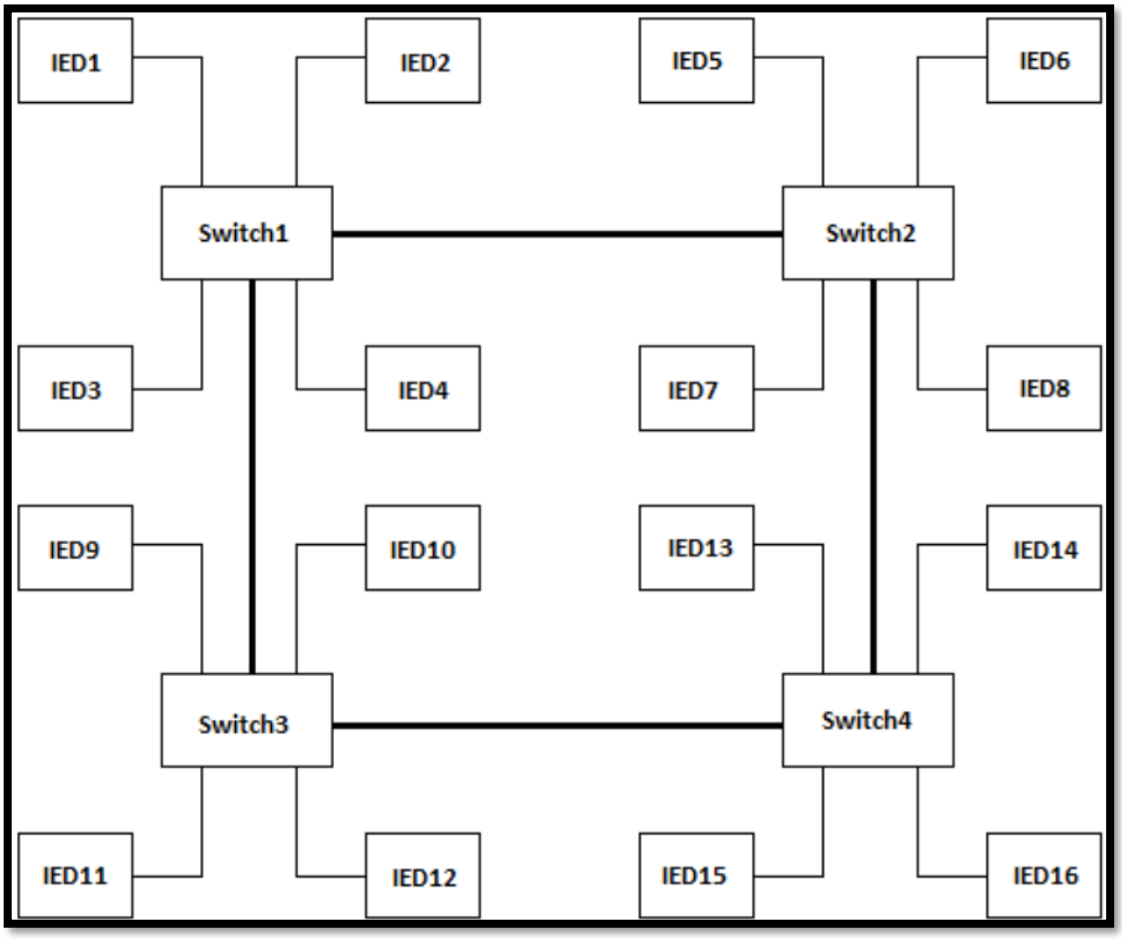
5.5 Topologia Mista

O uso de múltiplas configurações de anel e estrela é atraente ao examinar métodos de aplicação redundante para uma rede. Embora existam protocolos que facilitam arquiteturas físicas muito complexas, deve-se considerar a aplicação com

cuidado. Em arquiteturas que partem de uma topologia de anel simples, torna-se cada vez mais difícil, senão impossível, calcular com precisão o impacto da falha de um dos *switches* na rede. Em uma topologia de anel simples, a regra geral para um redirecionamento de protocolo (RSTP) é da ordem de 5 ms por *switch*. Em arquiteturas mais complexas, esse redirecionamento pode ser da ordem de minutos. (McDonald, 2012)

Uma das principais vantagens desta topologia é que a interligação em anel entre os *switches* agrega confiabilidade ao sistema, visto que numa situação de falha a conectividade lógica é mantida.

Figura 15. Topologia de Rede Mista

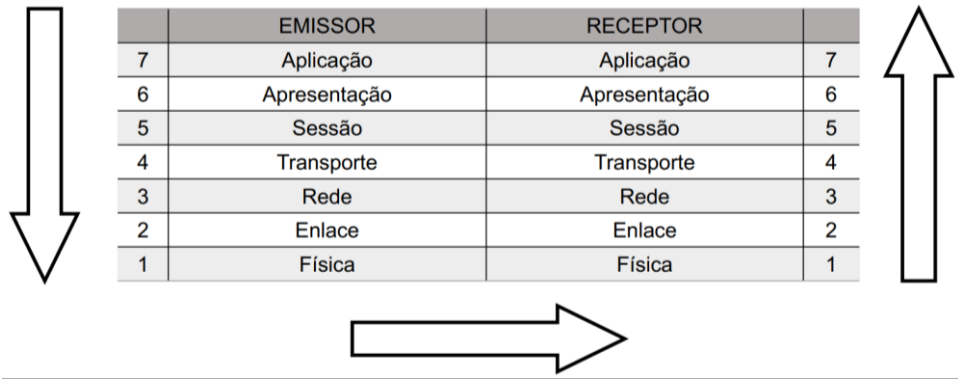


Fonte: (KREUTZ, 2014)

6 MODELO OSI

OSI (Open System Interconnection) é um sistema aberto e o padrão que serve como base para criação de protocolos de redes permitindo a comunicação entre dois sistemas quaisquer sem causar interferências nas suas lógicas internas. OSI é constituído por arquitetura hierárquica de sete camadas bem definidas, onde cada nível se comunica com o nível imediatamente acima ou abaixo, e cada nível é responsável por uma parte do processo de transferência de informações entre um sistema e outro. Os sete níveis que compõem o OSI são as seguintes:

Quadro 2. Níveis do modelo OSI



	EMISSOR	RECEPTOR	
7	Aplicação	Aplicação	7
6	Apresentação	Apresentação	6
5	Sessão	Sessão	5
4	Transporte	Transporte	4
3	Rede	Rede	3
2	Enlace	Enlace	2
1	Física	Física	1

Fonte: Autora

O quadro 2, mostra que quando um dispositivo está transmitindo dados, o fluxo de informação ocorre no sentido do *software* utilizado para a rede de comunicação. Portanto, os *softwares* se comunicam com a sétima camada, que por sua vez se comunicam com a sexta camada e assim por diante. Quando se está recebendo dados, o fluxo de informação ocorre no sentido oposto, ou seja, da rede de comunicação ao *software*.

6.1 Nível 1 (Físico):

O nível físico é responsável por transmitir um fluxo de *bits* num meio físico. Neste nível são definidas as características elétricas das interfaces entre os dispositivos, por exemplo: frequência, e níveis de pulsos ópticos ou elétricos e se o meio de transmissão será fibra óptica ou microondas.

Segundo Thomas e McDonald (2015), para que os dados sejam transmitidos, os dados do fluxo de *bits* devem ser convertidos em sinal elétrico ou óptico. Esta codificação também é definida pelo nível física, ele define a taxa de transmissão de dados, a sincronização dos *bits* no emissor e receptor, a conexão dos dispositivos à

mídia (ou seja, ponto a ponto ou multiponto), topologia física (como os dispositivos são conectados para fazer uma rede) e o modo de transmissão, simplex, half duplex ou full duplex.

6.2 Nível 2 (Enlace):

O nível de enlace de dados transforma os dados recebidos do nível rede em quadros de *bits* que trafegam na rede adicionando as informações de endereço da placa de rede de origem e destino. Segundo Thomas e McDonald (2015), este nível possui controle de fluxo, controle de erros e mecanismos de controle de acesso. O controle de fluxo evita o transbordamento do receptor com dados se a taxa de dados não for a mesma para o remetente e receptor. Além disso, é capaz de reconhecer se algum dos quadros estiver danificado, tiver se perdido e o reenviar.

Não havendo problemas, o quadro gerado é transmitido ao nível físico para ser transmitido pelo meio físico.

6.3 Nível 3 (Rede):

A camada de rede faz a entrega dos pacotes de mensagens do endereço de origem para o endereço de destino quando os dois sistemas estão conectados a redes diferentes. Se a comunicação for entre dispositivos que estão na mesma rede, não há necessidade de uma camada de rede. O endereçamento lógico e o roteamento são as principais funções do nível 3. Quando os dispositivos de comunicação estão em redes diferentes, para abordar os dispositivos de origem e destino, a camada de rede adiciona um cabeçalho nos dados do pacote. (Thomas e McDonald, 2015)

6.4 Nível 4 (Transporte):

O nível de Transporte segmenta os dados recebidos do nível de sessão em pacotes de dados menores que serão transmitidos pela rede. Quando o receptor recebe os dados do nível de rede ele remonta o dado original para então entregá-lo ao nível de sessão. Neste nível também é implementado o controle de fluxo e correção de erros nos dados através do envio de informações de reconhecimento ao transmissor, informando se determinado pacote foi recebido com êxito. Caso o dispositivo transmissor não receba uma confirmação de entrega de determinado pacote, este pacote deve ser reenviado.

6.5 Nível 5 (Sessão):

O nível de sessão controla o diálogo e a sincronização entre o emissor e receptor para estabelecer uma comunicação saudável. Para garantir a entrega adequada das mensagens ao receptor este nível realiza o processo de sincronização o qual é obtido através da divisão de um fluxo de dados num comprimento fixo e um ponto de verificação. Deste modo, ele reconhece a entrega dessas mensagens de forma independente, e em caso de perda, somente aquele comprimento específico de mensagem é retransmitido.

6.6 Nível 6 (Apresentação):

Neste nível são realizadas a tradução, criptografia e compactação de dados. Segundo Thomas e McDonald (2015), no processo de comunicação, a mensagem é convertida em fluxos de bits e, em seguida, transmitida, uma vez que diferentes sistemas usam diferentes métodos de codificação para os fluxos de bits, o nível de apresentação é necessário. Também podem ser implementados algoritmos de compreensão/criptografia.

6.7 Nível 7 (Aplicação):

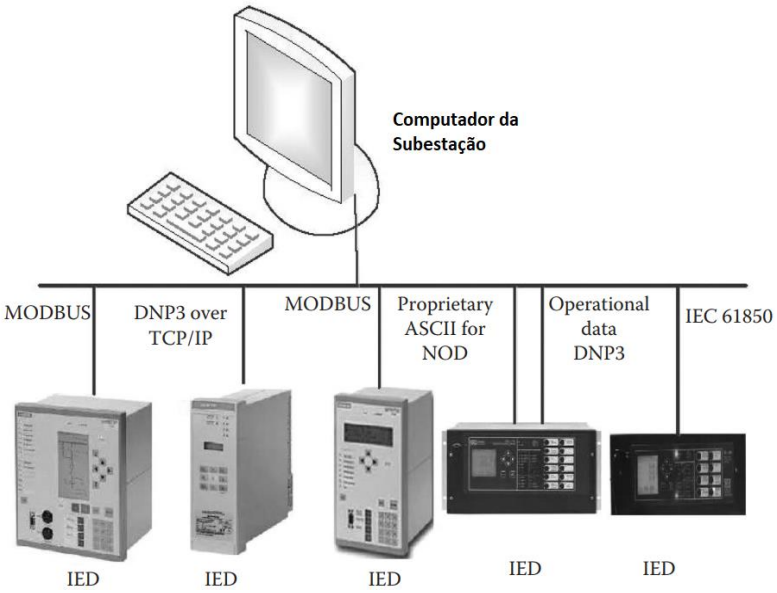
O nível de aplicação fornece a rede de acesso ao usuário, onde serviços como acesso e transferência de arquivos são fornecidos.

7 PROTOCOLOS DE COMUNICAÇÃO

Segundo McDonald (2012), ao trabalhar em automação de subestação e integração de sistemas, não há como evitar discussões em protocolos. Para garantir que os IEDs em uma subestação funcionem como um sistema, deve haver comunicação entre os dispositivos. Essa comunicação é geralmente por meio de fios de cobre ou cabos de fibra óptica (*wireless* não é comumente usado dentro da subestação devido a problemas com interferência e segurança). Os sinais são enviados por meio desses meios físicos usando sinais binários agrupados de acordo com um protocolo acordado.

Cada protocolo define uma série de regras sob as quais os dados podem ser transmitidos. Os protocolos mais utilizados nas comunicações das subestações estão explicitados abaixo.

Figura 16. Protocolos de comunicação do IED



Fonte: (Thomas e McDonald, 2015)

7.1 TCP/IP

TCP/IP é um protocolo de comunicação hierárquico baseado no modelo OSI, porém contém somente quatro níveis, sendo eles: Interface com a Rede, Rede, Transporte e Aplicação. Foi projetado para ser o protocolo utilizado na Internet. Sua principal característica é suportar a comunicação diretamente entre redes de diversos tipos.

A comunicação dos softwares ocorre na camada de aplicação utilizando protocolos de alto-nível, por exemplo: HTTP, FTP, Telnet. Após o processamento da requisição do *software*, o protocolo é enviado à camada de transporte, normalmente TCP. O nível de transporte é responsável por receber os dados do nível de aplicação e dividi-lo em pacotes para então enviá-los ao Nível de Rede. Cabe ainda ao Nível de Transporte na recepção dos dados, colocá-los em ordem e verificar se os mesmos estão intactos.

Segundo Covre (2011), no Nível de Rede encontra-se o protocolo IP, que recebe os dados da camada de Transporte e adiciona informações de endereçamento virtual. Em seguida, o pacote é enviado ao Nível de Interface com a Rede.

Quadro 3. Comparação entre Modelo OSI e TCP/IP

<table>
<tr><th></th><th>MODELO OSI</th><th>TCP/IP</th><th></th></tr>
<tr><td>7</td><td>Aplicação</td><td rowspan="3">Aplicação</td><td rowspan="3">4</td></tr>
<tr><td>6</td><td>Apresentação</td></tr>
<tr><td>5</td><td>Sessão</td></tr>
<tr><td>4</td><td>Transporte</td><td>Transporte</td><td>3</td></tr>
<tr><td>3</td><td>Rede</td><td>Rede</td><td>2</td></tr>
<tr><td>2</td><td>Enlace</td><td rowspan="2">Interface com a Rede</td><td rowspan="2">1</td></tr>
<tr><td>1</td><td>Física</td></tr>
</table>

Fonte: Autora

7.2 ModBus

O ModBus foi concebido para ser um protocolo de transferência de dados que atendesse aos CLPs e se tornou amplamente utilizado em aplicações industriais. É um protocolo do tipo Mestre/Escravo, ou seja, a comunicação é sempre iniciada pelo Mestre (os escravos nunca transmitem dados sem serem solicitados e não se comunicam entre si).

As transações podem ser de dois tipos: *Unicast* ou *Broadcast*. Na comunicação *Unicast*, o dispositivo mestre envia uma mensagem diretamente a um dos escravos, na comunicação *Broadcast* o mestre envia a mesma mensagem a todos os escravos. Um exemplo de mensagem Broadcast é o acerto de data e hora nos dispositivos pertencentes à rede. O Modbus usa as camadas 1, 2 e 7 do modelo OSI.

O protocolo determina o modo como um dispositivo escravo deve receber a mensagem endereçada a ele, determina o modo de ação e extrai as informações da mensagem recebida.

7.3 DNP3

O protocolo DNP3 (*Distributed Network Protocol 3*), também conhecido como IEEE Std 1815, é muito implementado nos sistemas de energia. O protocolo de rede distribuída (DNP3) é um dos mais adotados para comunicação entre subestações ou entre subestações e centros de controle. Um fator que contribuiu para sua popularização é ser um protocolo aberto, isto é, qualquer fornecedor tem acesso às suas informações para poder implementá-lo.

O DNP3 define dois tipos de estações: mestre e escravo. As estações escravas são equipamentos que aquisitam os dados e, quando solicitado pela estação mestre, transmite essas informações a estação mestre para que a mesma faça o processamento desses dados. As topologias adotadas neste protocolo são ponto-a-ponto, ponto-multiponto, hierárquica e concentrador de dados.

Na topologia ponto-a-ponto, existem somente uma estação escrava e uma estação mestre. Na topologia ponto-multiponto existe uma estação mestre e várias estações escravas, porém a comunicação entre mestre e escravos não é simultânea, ou seja, a estação mestre comunica-se com uma estação escrava por vez.

A topologia hierárquica permite que existam diversas estações mestre e escravas, porém cada estação escrava deve responder estritamente a seu mestre. Nesta topologia é possível que uma estação mestre tenha seus escravos e ao mesmo tempo seja escravo de uma estação mestre.

O protocolo DNP3 é dividido em cinco camadas, são elas: camada do usuário, de aplicação, de transporte, de enlace e física.

8 NORMA IEC 61850

Como citado anteriormente, até meados da década de 1990, havia poucos protocolos de comunicação abertos, de modo que cada fabricante definia e adotava os seus próprios protocolos de comunicação. Este fator dificultava a comunicação entre IEDs de fabricantes diferentes pois tornava necessária a inclusão de conversores de protocolos (*gateways*), contudo estes dispositivos tem atrasos inerentes e em ambientes que operam em tempo real, como é o sistema de automação de subestações estes atrasos podem gerar atuações indevidas.

O avanço de sistemas automatizados nas subestações trouxe a necessidade de desenvolvimento de um padrão de protocolos de comunicação aberto que permitisse a interoperabilidade entre IEDs, e em 2004 foi publicado o padrão internacional de Redes de Comunicação em Sistemas e Subestações IEC-61850.

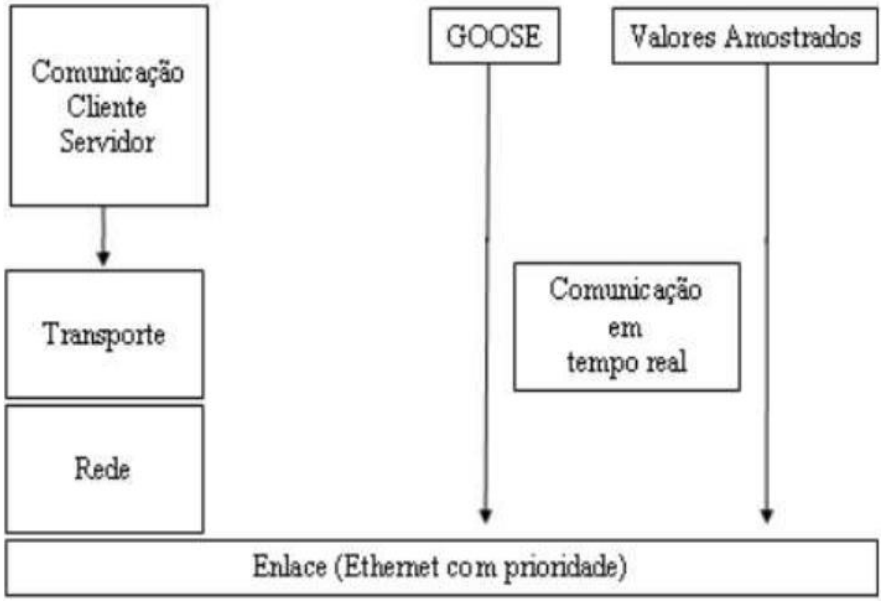
O desenvolvimento desta norma foi um dos principais marcos na evolução do sistema de automação de subestações. A IEC 61850 define a comunicação entre os dispositivos em uma subestação. Foi criada com o objetivo de normatizar a modelagem de dados, os barramentos de processo e os barramentos de estação, facilitando a interoperabilidade. Segundo Das (2018), os principais tópicos presentes na IEC 61850 são as seguintes:

- Definir tecnicamente os métodos de comunicação e especificar seus atributos;
- Recomendações para teste e comissionamento SAS;
- Diretrizes para controle e monitoramento de WAN;
- Estabelecer procedimento para comunicações entre subestações;
- Fornecer diretrizes para o gerenciamento de projetos de automação e engenharia de rede.

8.1 Tipos de Mensagens e Pilha de Protocolos

A pilha de protocolos é formada pelas camadas de transporte, rede e enlace. Somente a camada de enlace é comum a todas as mensagens e utiliza o e*thernet* com prioridade. As mensagens com restrição de tempo são mapeadas diretamente para a camada de enlace, enquanto as que não possuem restrição de tempo utilizam toda a pilha de protocolo.

Figura 17. Pilha de Protocolos



Fonte: (Gurjão, 2007)

8.1.1 Mensagens Cliente-Servidor

A norma IEC 61850 define três tipos de mensagem cliente-servidor: sincronização de tempo (tipo 6), serviços ACSI – *Abstract Communication Service Interface* (tipos 2, 3 e 5) e eventos genéricos do status da subestação – GSSE (*Generic Substation Status Event*) (tipos 1 e 1A). (Gurjão, 2007)

São utilizadas para troca de informações com o intuito de indicar status de um determinado equipamento. Esse protocolo emprega o modelo TCP, não sendo indicado para atuação de proteção.

8.1.2 Mensagens GOOSE e Valores Amostrados

São mensagens *multicast* que carregam informações entre IEDs. Informam a atuação das proteções existentes. Empregam o padrão UDP, não fazendo verificação para identificar se a mensagem emitida chegou ao receptor sem erros. A mensagem emitida é repetida até que o receptor sinalize o recebimento.

O protocolo SV (*Sampled Variables*) é responsável pelo tráfego das leituras analógicas da subestação. Através desse protocolo, TPs e TCs conseguem enviar suas medições para os relés através de leituras digitais pela própria rede ethernet. Os relés, por sua vez, com um conversor AD incorporado, tratam esse dado e o utilizam em suas proteções. Por esse motivo, pertencem ao tipo 1 da tabela da figura 18.

Figura 18. Tipos de Mensagens e Classes de Desempenho

Tipo	Classe
1	Mensagens rápidas
1A	Trip
2	Velocidade média
3	Baixa velocidade
4	Dados em rajada (*raw data*)
5	Transferência de arquivos
6	Sincronização de tempo

Fonte: (Gurjão, 2007)

9 AMEAÇAS CIBERNÉTICAS AO SISTEMA DE AUTOMAÇÃO DE SUBESTAÇÕES

Nas últimas décadas a evolução tecnológica dos IEDs, tornou possível um acréscimo de funcionalidades de proteção e controle agrupadas num mesmo dispositivo em comparação com as soluções adotadas anteriormente. Além disso, houve a introdução das redes locais (LAN) no controle dos módulos que compõem a subestação, em substituição ao cabeamento de cobre.

Os padrões de comunicação definidos na IEC 61850, vem se tornando a base dominante nos sistemas de proteção e automação não somente em trocas de informações internas à subestação, mas também entre subestações ou entre uma subestação e o centro de operação de subestações. A adoção da automação trouxe como desvantagem a vulnerabilidade a interferência maliciosa ou ataque de duas fontes:

- Interferência Eletromagnética Intencional;
- Ataques Cibernéticos.

A evolução das telecomunicações nos sistemas de proteção e controle vem permitindo o uso de tecnologias mais flexíveis e de maior performance. A segurança cibernética é o novo desafio que surge dessas novas tecnologias. Tem sido exigido dos fabricantes que identifiquem os pontos de vulnerabilidades de seus produtos e se adaptem rapidamente para atender aos requisitos de segurança cibernética, principalmente equipamentos relacionados à tecnologia da informação (TI) e rede (por exemplo; roteador de *switches*, *firewalls*, etc.).

Um sistema de automação vulnerável coloca em risco os pilares que sustentam um sistema cibernético bem projetado: confidencialidade, integridade e disponibilidade.

O CIGRE - Conselho Internacional de Grandes Sistemas Elétricos (2014) agrupa em quatro categorias os possíveis ataques cibernéticos destinados a uma subestação, são elas: bloqueio, imitação e modificação e coletivos. Os ataques podem ocorrer de modo independente ou em conjunto. O resultado é a perda de ao menos um dos três fatores chaves que devem ser atendidos em todo sistema cibernético: confidencialidade, integridade e disponibilidade.

Na categoria de ataques por bloqueio é possível se identificar quatro tipos de ataque: *Denial of Service* (DoS), *Jamming*, *Fuzzing* e *Malware*. O objetivo principal neste tipo de ataque é causar obstrução na rede através de sobrecarga no fluxo de dados.

Negação de Serviço, também conhecido como DoS (*Denial of Service*), é um ataque que procura tornar os dispositivos nos quais se hospeda indisponíveis. Não é considerado uma invasão ao sistema, mas sim uma invalidação causada por sobrecarga. Os ataques DoS normalmente ocorrem de duas formas: Consome todos os recursos de memória ou processamento de forma que o sistema não é mais capaz de fornecer seus serviços ou obstrui a mídia de comunicação entre dispositivos e o sistema vítima do ataque é incapaz de se comunicar adequadamente. Como consequência há uma invalidação dos dados transmitidos e pode ser evitado com a inclusão de firewalls (*software* responsável pelo controle do tráfego de dados na rede), roteadores e *proxys* de serviço.

Jamming é uma interferência eletromagnética causada pela emissão de um sinal que possui frequência semelhante à frequência na qual os dados estão sendo transmitidos. O *Jamming* causa invalidação dos dados e pode ser evitado através de dispositivos *anti-jamming*.

O ataque *fuzzing*, também conhecido como ataque por força bruta, ocorre através da emissão de mensagens aleatórias e inesperadas com o objetivo de testar inúmeras permissões de acesso usando a abordagem de tentativa e erro a fim de descobrir as senhas de acesso e usuários de um determinado sistema ou dispositivo.

Entre os ataques existentes na categoria de imitação e modificação estão os ataques por falsificação, adulteração e repetição.

Em ataques por falsificação o invasor, seja uma pessoa ou programa, se identifica como um usuário legitimo para obter vantagens de acesso. Pode ocorrer em protocolos nos quais não há identificação de origem ou destino de uma mensagem, caso não sejam aplicadas verificações de identidade.

A adulteração ocorre quando os dados são modificados deliberadamente (destruídos, manipulados ou editados) por meio de canais não autorizados. Os dados existem em dois estados: em trânsito ou em repouso. Em ambos os casos, os dados podem ser interceptados e adulterados. Por exemplo, nos casos em que os pacotes de dados são transmitidos sem proteção, um invasor não autorizado pode interceptar

o pacote de dados, modificar seu conteúdo e alterar seu endereço de destino. Com os dados em repouso, um aplicativo do sistema pode sofrer uma violação de segurança e um invasor não autorizado pode implantar um código malicioso que corrompe os dados ou o código de programação subjacente

Ataque por repetição é uma forma de ataque à rede em que a transmissão de dados válidos é maliciosa ou fraudulentamente repetida ou atrasada. Isso é realizado pelo invasor que intercepta os dados e os retransmite.

Na categoria de ataques coletivos, tem-se ataques de espionagem e análise de tráfego.

Um ataque de espionagem ocorre quando um invasor intercepta, exclui ou modifica dados que são transmitidos entre dispositivos. A espionagem depende de comunicações de rede não seguras para acessar dados em trânsito entre os dispositivos.

A definição de ataque por espionagem, normalmente ocorre quando um usuário se conecta a uma rede na qual o tráfego não está protegido ou criptografado e envia dados comerciais confidenciais a outro usuário. Os dados são transmitidos por uma rede aberta, dando ao invasor a oportunidade de explorar uma vulnerabilidade e interceptá-la por meio de vários métodos.

Uma análise de tráfego é o processo de interceptar e examinar mensagens para deduzir informações de padrões de comunicação, o que pode ser realizado mesmo quando como mensagens estão criptografadas. Em geral, quanto maior o número de mensagens observadas, ou mesmo interceptadas e armazenadas, mais se pode inferir do tráfego.

10 ESTUDO DE CASO

Neste capítulo será analisada a arquitetura de rede e o sistema de automação de uma subestação com o intuito de observar os conceitos previamente expostos. A empresa responsável pela subestação possui uma política interna de não divulgação dos dados técnicos de suas instalações. Deste modo, os dados expostos, que são objetos deste estudo, foram modificados a fim de preservar a privacidade da instalação sem gerar prejuízos as análises efetuadas.

10.1 Dados da Instalação

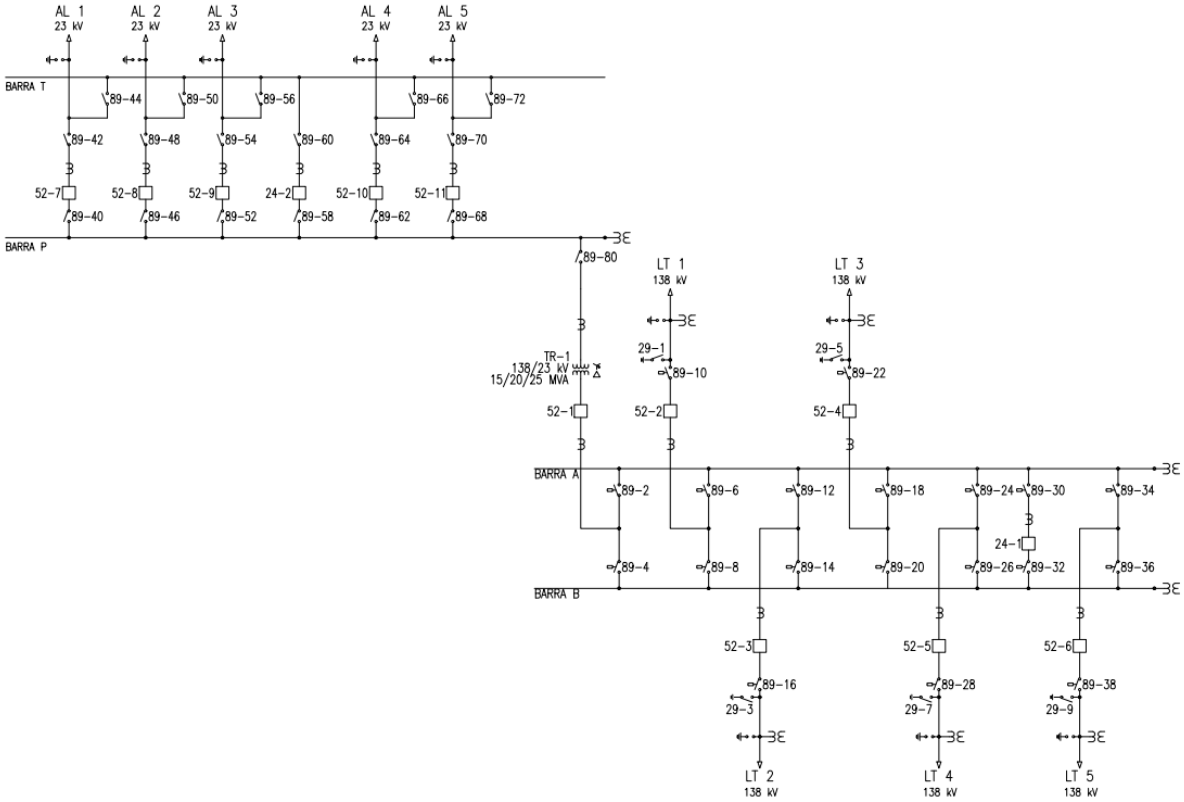
A subestação em análise é de médio porte e pertence a uma empresa transmissora de energia. Está subestação possui fronteira com a subestação elevadora de uma usina hidrelétrica.

O arranjo dos barramentos é do tipo barra-dupla 4 chaves, porém a seccionadora de contorno será instalada futuramente. Possui 5 linhas de transmissão operando na tensão de 138 kV, um módulo de transferência no setor em 138 kV e um transformador de força de 15/20/25 MVA (ONAN/ONAFI/ONAFII) utilizado para rebaixar a tensão de 138/23 kV.

O setor de 23 kV possui o arranjo de barra principal e transferência com seis módulos de alimentadores e um módulo de transferência.

Essa subestação possui no seu setor 138 kV um robusto sistema de oscilografia nos qual são registrados correntes, tensões e disparos ocorridos por funções de proteção. Esse sistema de oscilografia é independente dos registros feitos nos IEDS de proteção dos módulos pois oferece, em caso evento, uma visão abrangente e mais confiável do ocorrido.

Figura 19. Diagrama Unifilar



Fonte: Autora

10.2 Sistema de Proteção e Controle

Apesar do nível de tensão máximo no qual essa subestação opera (138kV) não ser considerado como Rede Básica, as suas proteções foram implementadas atendendo ao submódulo 2.6 - Requisitos mínimos para os sistemas de proteção e de telecomunicações do ONS.

A solução de proteção adotada nessa subestação é da fabricante *Schweitzer Engineering Laboratories* – SEL. A SEL oferece IEDs de proteção específicos para cada aplicação, conforme detalhado a seguir:

10.2.1 SEL 411L - Proteção e Controle de Linhas

Esse IED de proteção foi aplicado pois é capaz de executar as funções de proteção de distância, diferencial de linha, sincronismo, religamento, falha disjuntor, sobrecorrente, sobrecorrente temporizada e sobrecorrente direcional. Possui portas seriais e portas ópticas *ethernet*, sendo compatível com os protocolos SEL, DNP3, *ModBus* e IEC61850.

10.2.2 SEL 487E - Proteção e Controle de Transformador

Esse IED de proteção foi aplicado pois é capaz de executar as funções de diferencial de transformador, sincronismo, falha disjuntor, sobrecorrente, sobrecorrente temporizada e sobrecorrente direcional. Possui portas seriais e portas ópticas *ethernet*, sendo compatível com os protocolos SEL, DNP3, *ModBus* e IEC61850.

10.2.3 SEL 2414 – Controle e Monitoramento de Transformador

Esse relé é responsável por fazer as funções de monitoramento de temperatura, regulação de tensão e controle da ventilação forçada do transformador de potência. Possui de IED possui portas seriais e portas ópticas *ethernet*, sendo compatível com os protocolos SEL, DNP3, *ModBus* e IEC61850.

10.2.4 SEL 487B - Proteção de Barras

Esse IED de proteção foi aplicado pois é capaz de executar as funções de diferencial de barra, falha disjuntor, sobrecorrente e sobrecorrente temporizada. Possui portas seriais e portas ópticas *ethernet*, sendo compatível com os protocolos SEL, DNP3, *ModBus* e IEC61850.

10.2.5 SEL 2440 – Controle

Este IED não executa funções de proteção. É um equipamento que executa funções de controle, sendo composto somente por entradas e saídas digitais. Possui portas seriais e portas ópticas *ethernet*, sendo compatível com os protocolos SEL, DNP3, *ModBus* e IEC61850.

10.3 Vulnerabilidades no Sistema de Automação

10.3.1 Senhas de Acesso

As senhas de acesso são medidas importantes de segurança. Criar uma senha bem estruturada é uma ótima defesa contra invasões ao sistema. Por exemplo: a manutenção das senhas padrão de fábrica dos relés de proteção para acessos de níveis 1 e 2, no caso do fabricante SEL senhas: OTTER e TAIL, respectivamente aumenta a vulnerabilidade.

A regulamentação NERC-CIP existente pede que as senhas adotadas nos dispositivos e sistemas de automação de subestações possuam, ao menos, seis

caracteres combinando letras, números e caracteres especiais e que esta senha seja modificada anualmente ou com menor frequência.

10.3.2 Utilização de Contas Globais

A utilização de contas globais traz vulnerabilidade ao SAS, pois perde-se a capacidade de determinar qual usuário fez determinado acesso ou modificação, visto que existe mais de um usuário com a informação da senha.

A solução para esse tópico é a criação de senhas individuais.

10.3.3 Autenticação

A autenticação é a validação do usuário através de sua identidade no sistema, ou seja, através do seu nome de usuário, senha e endereço de IP. A falta de procedimento de autenticação deixa o sistema vulnerável, pois uma pessoa não autorizada que tenha conhecimento sobre o *login* e senha de um usuário é capaz de acessar áreas de acesso restrito.

10.3.4 Autorização

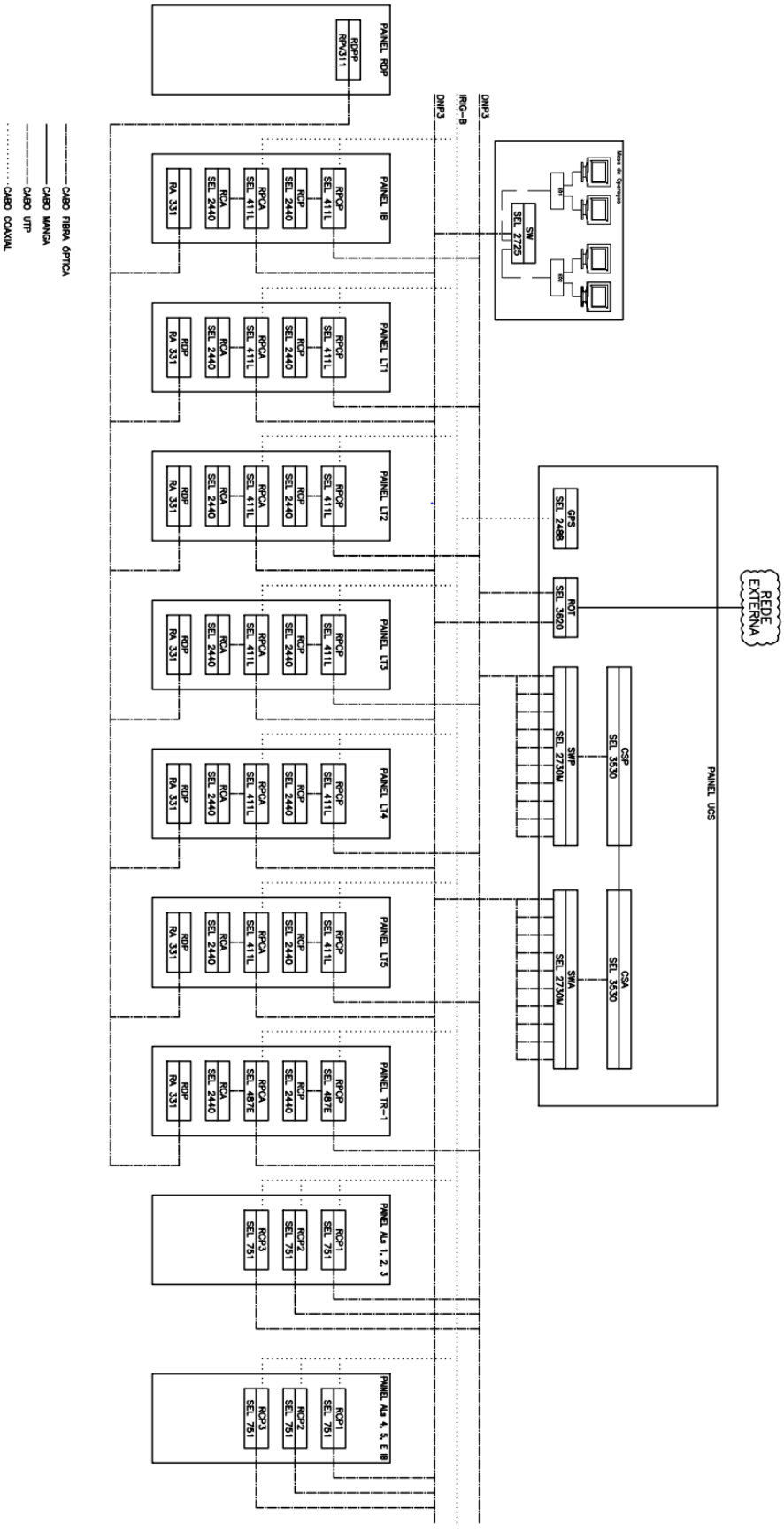
Autorização é um conjunto de permissões dadas a um usuário do sistema. Manter o acesso aos dados do sistema disponível a todos os usuários não é seguro, devido a usuários poderem, ainda que por acidente, desconfigurar parâmetros que eles sequer precisariam ter acesso, pois não são os responsáveis.

A solução é limitar os níveis de acessos dos usuários as funções que eles exercem.

10.3.5 Rastreabilidade

Sem rastreabilidade é impossível buscar o responsável por alguma alteração indevida. Pois num sistema com rastreabilidade os dados referentes as alterações feitas ficam armazenados juntamente com os nomes de usuários, senhas, datas e horários.

Figura 20. Arquitetura de Comunicação



Fonte: Autora

11 CONCLUSÕES

Num sistema tão complexo e relevante como é o sistema de energia o resultado de uma invasão ao sistema de automação de uma subestação pode ser inimaginável. O sucesso dos possíveis ataques é determinado pela combinação das deficiências no sistema. Deste modo, identificar e mitigar as fragilidades do sistema de automação é fundamental.

Percebe-se que a segurança deve fazer parte da cultura empresarial, no sentido que deve ser um compromisso de todos na empresa. Inúmeros procedimentos podem ser adotados visando precaver um ataque cibernético como: a adoção de senhas fortes, acessos restritos aos níveis cabíveis a determinados usuários e auditoria dos logins efetuados, bem como das alterações feitas durante esses acessos, utilização de criptografia para os enlaces externos, roteadores, *firewalls* e antivírus. Adoção de *whitelist*, uma lista de permissões na qual o padrão é o “acesso negado” sendo permitido acesso somente aos componentes da *whitelist* nos equipamentos com tarefas em tempo real. Desabilitação de portas ociosas em *switches* para evitar conexões não autorizadas.

As ferramentas citadas são simples e podem ser implementadas tanto em subestações automatizadas existentes ou novas tornando o sistema de automação dessa instalação menos vulnerável a ataques cibernéticos.

12 REFERÊNCIAS

OLIVEIRA Carlos; ABBOUD, Ricardo. **Desafios da segurança cibernética nas subestações de energia elétrica**. 91ª Edição. Revista: O Setor Elétrico. 2013.

COLBERT, Eduard J. M.; KOTT, Alexander. **Cyber-Security of SCADA and Others Industrial Control System**. 1ª Edição. Fairfax, USA: Springer, 2016.

COVRE, Helber Peixoto. **Integração de Dados dos Sistemas de Proteção de Subestações Distribuidoras**. Tese (Mestrado) – Escola Politécnica, Universidade de São Paulo. São Paulo, p. 114, 2011.

GURJÃO E.C., SOUZA B.A. e CARMO U. A. **Aspectos de Comunicação da Norma IEC-61850**. João Pessoa – PB. 2007

International Council on Large Electric Systems (CIGRE). **Substations**. Paris, Fança, 2019.

KREUTZ, Felipe de Campos. **Automação de Subestações através da norma IEC 61850**. Monografia (Graduação) – Departamento de Engenharia Elétrica, Universidade Federal do Rio Grande do Sul. Porto Alegre, p. 66, 2014.

MAMEDE, João. **Subestações de Alta Tensão**. 1ª Edição. Rio de Janeiro, Brasil: Gen LTC, 2021.

MAMEDE, João. **Manual de Equipamentos Elétricos**. 1ª Edição. Rio de Janeiro, Brasil: Gen LTC, 2013.

McDONALD, John D. **Electric Power Substations Engineering**. 3ª Edição. Boca Raton, USA: CRC Press, 2012.

NOUH, Dazahra e outros. **A Defense-in-Depth Cybersecurity for Smart Substation**. Marrocos: Institute of Advanced Engineering and Science, 2018.

THOMAS, Mini S.; McDONALD, John D. **Power System SCADA and Smart Grids**. 1ª Edição. Boca Raton, USA: CRC Press, 2015.

R. DOROTHY, Sasilatha, **Smart Grid Systems Based Survey on Cyber Security Issues**, Bulletin of Electrical Engineering and Informatics ,Vol. 6, No. 4, December 2017.

ROBERTO, Wesley**. Segurança Cibernética para Subestações: Implementado Ferramenta Simples e Eficaz.** SEL Webinar. Campinas. 2020